Testimony of

The Electronic Transactions Association

Before the

House Committee on the Judiciary

Subcommittee on Regulatory Reform, Commercial and Antitrust Law

Hearing on

"Guilty until Proven Innocent? A Study of the Propriety & Legal Authority for the Justice Department's Operation Choke Point."

July 17, 2014

Testimony Made by

Scott Talbott

Senior Vice President of Government Affairs

The Electronic Transactions Association

Chairman Bachus, Ranking Member Johnson and Members of the Subcommittee, the Electronic Transactions Association (ETA) appreciates the opportunity to submit this statement for the record for the House Judiciary Committee's Subcommittee on Regulatory Reform, Commercial and Antitrust Law's hearing, "Guilty until Proven Innocent? A Study of the Propriety & Legal Authority for the Justice Department's Operation Choke Point."

ETA is an international trade association representing companies that offer electronic transaction processing products and services related to debt, credit, and prepaid cards. The purpose of ETA is to grow the payments industry by providing leadership through education, advocacy, and the exchange of information. ETA's membership spans the breadth of the payments industry, from financial institutions to transaction processors to independent sales organizations to equipment suppliers. More than 500 companies worldwide are members of ETA.

Keeping Fraud Off Payment Systems

ETA strongly supports the vigorous enforcement of existing laws and regulations to prevent fraud. Consumers in the United States choose electronic payments over cash and checks because they have zero liability for fraud, making electronic payments the safest and most reliable way to pay. As a result, payment companies are generally responsible for paying for fraud involving payment systems under Federal law and payment network rules, and thus our members have a strong interest in making sure fraudulent actors do not gain access to payment systems. With the benefit of decades of payment system expertise, ETA members have developed effective due diligence programs to prevent fraudulent actors from accessing payment systems and to terminate access for network participants that engage in fraud. These programs have helped to

keep the rate of fraud on payment systems at remarkably low levels. In 2012, there was more than $4.6 trillion in debit, credit and prepaid card transactions in the United States, but there was only $5.5 billion in credit card fraud. In addition, a recent survey of ETA members indicates that more than 10,000 merchants were discharged last year for fraud. These actions demonstrate the commitment of ETA members to keeping fraudulent actors off payment systems.

Despite this strong record, however, payment processors can never take the place of regulators and law enforcement in protecting consumers. Because regulators and law enforcement can issue subpoenas, conduct investigations, and have far great resources, personnel, and legal authorities, they will always be in a far better position to combat fraud. Yet, payments companies are committed to doing their part.

ETA therefore believes we must be constantly vigilant on continuing to update our processes. The growth of internet commerce has created remarkable new opportunities for business and benefits for consumers, but unfortunately also has created new opportunities for fraud. For example, because websites can change in the blink of an eye, they can be difficult to monitor and easy for fraudsters to exploit. Hence, ETA welcomes further Federal efforts to combat fraudulent activity by unscrupulous merchants that operate on the internet.

In an effort to further strengthen payment systems, ETA has recently published new industry guidelines for merchant due diligence and monitoring that provide more than 100 pages of methods and practices to detect and halt fraudulent actors. The ETA Guidelines were developed by ETA's member companies after months of discussions and sharing of techniques to prevent

fraud. During this process, ETA even shared the preliminary draft guidelines with, and sought comments from, the Federal Trade Commission (FTC), which had strongly encouraged the industry to strengthen its anti-fraud efforts. Now, ETA is actively encouraging its members and companies across the payments ecosystem to make use of the guidelines, especially smaller companies that may not have the resources to develop such advanced practices on their own.

The ETA Guidelines provide a practical and targeted approach to combating fraud on payment systems. ETA members already have a strong commitment to, and financial interest in, keeping fraudulent actors off payment systems, but the targeted nature of the ETA Guidelines gives them enhanced tools to improve their effectiveness and help ensure that law-abiding merchants do not unfairly lose access to payment systems due to overly broad anti-fraud protections.

Another benefit of the ETA Guidelines is that they provide a basis for payments companies to work cooperatively with Federal regulators and law enforcement toward their common goal of stopping fraud. ETA strongly believes that such a collaborative approach is good public policy. It would encourage companies to cooperate with law enforcement by fostering an environment of open communications between government agencies and payments companies. As a result, such a cooperative approach would be more effective at protecting consumers from fraud.

Concerns About Operation Choke Point

Unfortunately, the Department of Justice (DOJ) and other Federal regulators have begun pursuing a more confrontational approach to addressing fraud on payment systems. On March 20, 2013, the Financial Fraud Enforcement Taskforce publicly announced a new initiative by its

Consumer Protection Working Group (which is co-chaired by representatives from the DOJ, the FTC, and the Consumer Financial Protection Bureau) to address mass consumer frauds by holding banks and payment processors liable for the acts of certain merchants.[1] This initiative, named "Operation Choke Point" by the DOJ, aims to "close the access to the banking system that mass marketing fraudsters enjoy – effectively putting a chokehold on it."[2]

Although ETA strongly supports increased law enforcement aimed at preventing mass frauds, it has serious concerns about the Operation Choke Point approach. In ETA's view, Operation Choke Point employs the wrong legal tools, is unnecessarily confrontational, and creates serious risks to law abiding processors and merchants without producing any benefits to consumers beyond those which could be obtained with a more focused and collaborative approach.

The DOJ has sought to implement Operation Choke Point by initiating investigations and civil suits under the Financial Institutions Reform, Recovery, and Enforcement Act, 12 U.S.C. § 1833a (FIRREA). Under FIRREA, the DOJ can initiative investigations and bring civil suits for alleged violations of 14 predicate criminal offenses, including wire fraud "affecting a federally-insured financial institution."[3] Several courts have recently held that FIRREA suits can be brought against not only third parties whose violations "[affect] a federally-insured financial institution," but also against the banks whose violations affect themselves.[4] This broad reading of FIRREA has given DOJ a very powerful tool because under FIRREA the statute of limitations

[1] http://www.justice.gov/iso/opa/doj/speeches/2013/opa-speech-130320.html.
[2] *Id.*
[3] 12 U.S.C. § 1833a(c)(2).
[4] United States v. Bank of New York Mellon, 941 F. Supp. 2d 438 (S.D.N.Y. 2013); United States v. Countrywide Fin. Corp., 961 F. Supp. 2d 598 (S.D.N.Y. 2013); United States v. Wells Fargo Bank, N.A., 972 F. Supp. 2d 593 (S.D.N.Y. 2013).

is 10 years and cases only need to be proven by "preponderance of the evidence," rather than the "beyond a reasonable doubt" standard required in criminal prosecution.[5] In addition, FIRREA provides for penalties of up to $5 million for each violation or, if greater, the amount of any pecuniary gain derived by the violation or of any losses inflicted on another person.[6] These provisions significantly tilt the litigation playing field in favor of the DOJ and make FIRREA cases very costly for companies to defend against and risky to litigate.

It is important to note that FIRREA was not designed to address mass frauds. It was passed to reform the regulatory regime for thrifts in the wake of the S&L Crisis of the 1980s. The purpose of Section 1833a was to protect the government from financial frauds. Hence, Section 1833a provides the Federal government with enhanced authority to pursue claims against individuals for fraudulent actions that directly harm the Federal government or harm financial institutions insured by the Federal government. It is not a consumer protection statute, which is demonstrated by the fact that FIRREA penalties do not redress consumer injury, but instead get paid to the U.S. Treasury. Therefore, the use of FIRREA for consumer protection purposes is a case of the wrong tool being used for the right goal.

Although no court has yet issued a final decision in a FIRREA case involving payment processing, DOJ has recently settled two FIRREA cases involving payment processing and issued scores of subpoenas to financial institutions as part of Operation Choke Point. These settlements, combined with recently released DOJ memoranda detailing the agency's plans for Operation Choke Point, have raised concerns among ETA's members that Operation Choke Point

[5] 12 U.S.C. § 1833a(f), (h).
[6] 12 U.S.C. § 1833a(b).

will result in the government seeking to broaden the scope of processor liability for the acts of merchants.[7] There is also concern that Operation Choke Point will be used to impose penalties on financial institutions for processing transactions of certain categories of legal but disfavored businesses.

The problems with Operation Choke Point are not limited to the DOJ. ETA is also concerned that other Federal regulators are considering following the DOJ's lead and adopting additional initiatives modeled on Operation Choke Point. ETA's members have reported a sharp increase in information requests and civil investigative demands from the FTC. In light of the DOJ's implementation of Operation Choke Point and recently released DOJ memorandum indicating FTC involvement with the development of Operation Choke Point, the FTC's increased interest in payment processing has sparked concerns that the FTC has begun its own Operation Choke Point. [8]

Currently, the FTC can assert jurisdiction over payment processors that engage in unfair or deceptive acts or practices in violation of Section 5 of the Federal Trade Commission Act, and violations of the Telemarketing Sales Rule.[9] The FTC also can bring cases against payment processors for "assisting and facilitating" a merchant's violations of the Telemarketing Sales

[7] The Department of Justice's "Operation Choke Point": Illegally Choking Off Legitimate Businesses?, U.S. House of Representatives, Committee on Oversight and Government Reform, Staff Report (May 29, 2014), Appendix 1.
[8] *Id*. (The DOJ has indicated that it is making "significant efforts to engage other agencies," including the FTC. The DOJ also has noted that "[t]he FTC's efforts in this area predate our own, and not surprisingly our agencies work closely together." (Memorandum dated November 21, 2013 to Staff of the Office of the Attorney General et. al. from Maame Ewusi-Mensah Frimpong, Deputy Assistant Attorney General, Civil Division. Subject: Operation Choke Point, p. 12)).
[9] 15 U.S.C. § 45; 16 C.F.R. § 310.

Rule, but such liability only applies if a payment processor "knows or consciously avoids knowing" that the merchant violated the rule. [10]

ETA fully supports the proper enforcement of these statutes by the FTC, but is concerned that the FTC is looking to change its long-standing policy of pursuing only processors that were actively engaged in assisting a merchant in committing fraud or avoiding detection. To the extent the FTC begins premising liability on nothing more than providing a merchant an account, or deems high return rates to be constructive knowledge of fraud, it will be dramatically altering the liability scheme for payment processing in a manner that could have significant, adverse consequences.

Impact of Operation Choke Point on Processors, Entrepreneurs, and Consumers

From a public policy perspective, Operation Choke Point and any similar efforts by the FTC or other regulators to impose enhanced liability on payment processing will likely have adverse consequences for not only merchants and entrepreneurs, but also the very consumers Operation Choke Point purports to protect. In addition, Operation Choke Point sets a troubling precedent of government agencies using the payment systems to achieve objectives unrelated to preventing financial fraud.

First, if payment companies' liability for the actions for merchants increases, processors may very well have little choice but to increase the prices of payment services for merchants and/or restrict access to their payment systems to manage their new liability exposure. Invariably, the

[10] 16 C.F.R. § 310.3

brunt of these burdens will fall on small, new and innovative businesses because they pose the highest potential risks. For example, start-up internet businesses with liberal return policies present high risks to financial institutions because they have no transaction history, rely on card-not-present transactions and have (by design) high return rates. Federal regulators view high return rates as strong evidence of fraud. Due to the risks these new businesses present, banks and payment processors may very well decide that the increased liability risks outweigh the benefits of having them as customers. Because in today's marketplace consumers expect merchants to accept debit, credit, and prepaid cards, the inability of a merchant to access the payment systems could effectively be the death knell for its business. New restrictions on access to payment systems, or even higher costs to access payment systems, could therefore become an impediment to job creation and innovation, especially in the critical high-tech start-ups and internet commerce segments of the economy.

Second, increasing liability on payment processing, especially processing of debit, credit, and prepaid cards, does not necessarily benefit consumers. It is consumers who will ultimately pay for the higher costs arising from increased liability. They also will be harmed by the inconvenience of not being able to use their preferred methods of payment (credit, debit, and prepaid cards) with some merchants due to more restrictive access to payment systems. Similarly, they would be harmed if new liability on processors impedes continued innovations in electronic payments. Over the last twenty years, electronic transactions have grown rapidly to become the dominant method of payment for consumer transactions due to their convenience, security (especially when compared to cash), and customer service. Therefore, to the extent that

new liability risks impede the evolution of electronic transactions, consumers will have less access to the payment methods they prefer and beneficial developments in electronic payments.

Third, there is a real risk that a confrontational approach, like Operation Choke Point, will alter payments companies' natural incentive to cooperative with law enforcement and regulatory authorities if they believe that such cooperation will only result in enforcement actions against them. Thus, a far better approach would be to establish a reasonable safe harbor that would allow payments companies, which were not directly involved in the fraudulent activities of a merchant, to work with regulators without any risk of triggering an enforcement action. ETA believes that such cooperation between payments companies and regulators is likely to be more effective because it recognizes and further strengthens the strong incentives such companies already have to prevent fraudulent actors from accessing payment systems. This conclusion (as well as further analysis of the adverse consequences arising from imposing additional liability on payment processors) was also the result of a recent study by NERA Economic Consulting commissioned by ETA, which is attached as Exhibit A.

Finally, enforcement actions against payment systems are an inappropriate tool for regulators to use to limit the ability of consumers to access legal but currently disfavored industries. There has been much debate about the attempts by Operation Choke Point and similar regulatory efforts to compel payments companies to sever relationships with a variety of legal but disfavored industries, ranging from coin dealers and short-term lenders, to home-based charities and pharmaceutical sales.[11] ETA believes that such efforts unfairly expose institutions to

[11] *See* The Department of Justice's "Operation Choke Point": Illegally Choking Off Legitimate Businesses?, U.S. House of Representatives, Committee on Oversight and Government Reform, Staff Report (May 29, 2014), p. 8.

regulatory actions merely for engaging in lawful commerce. Moreover, if the precedent is set that regulators can unilaterally intervene to keep certain lawful industries off payment systems, payments companies will be subject to shifting regulatory exposure as the disfavored industries of regulators shifts with changes in administrations and agency personnel. If regulators have concerns about a particular industry, the appropriate forums for addressing those concerns are formal rulemakings, Congress, or state legislatures. To be clear, ETA takes no position on which types of industries should be legal and its members are fully committed to preventing any businesses engaged in activities prohibited by statute or regulation from accessing payment systems. ETA merely seeks to ensure that payments companies can freely process transactions for any law-abiding merchant.

Conclusion

Operation Choke Point is premised on the flawed assumption that increasing liability on lawful payments companies for the actions of fraudulent merchants will yield only benefits to consumers. In practice, however, imposing new liability standards on such institutions is likely to have serious adverse consequences for not only law-abiding merchants, but also consumers generally. There needs to be a careful balancing of the need to limit access to payment systems to prevent fraud and the need to ensure that all law-abiding businesses can access the payment systems consumers want to use. A cooperative approach to combating fraud by financial institutions and Federal regulators is far more likely to strike the right balance than blunt enforcement actions. Accordingly, ETA stands ready to work with federal regulators to work cooperatively toward our common goal of preventing fraud.
